

Implementation of Grover's Quantum Search Algorithm in a Scalable System

K.-A. Brickman, P. C. Haljan, P. J. Lee, M. Acton, L. Deslauriers, and C. Monroe
FOCUS Center and Department of Physics, University of Michigan, Ann Arbor, MI 48109

(Dated: February 1, 2008)

We report the implementation of Grover's quantum search algorithm in the scalable system of trapped atomic ion quantum bits. Any one of four possible states of a two-qubit memory is marked, and following a single query of the search space, the marked element is successfully recovered with an average probability of 60(2)%. This exceeds the performance of any possible classical search algorithm, which can only succeed with a maximum average probability of 50%.

PACS numbers:

Quantum computers promise dramatic speedup over conventional computers in some applications owing to the power of entangled superpositions [1]. Among the best-known quantum applications is Grover's search algorithm, which can search an unsorted database quadratically faster than any known classical search [2]. A common analogy for this searching algorithm is the problem of finding a person's name in a phone book given only their phone number [3]: for N entries in the phone-book, this requires of order N queries. However, if the correlation between name and phone number is encoded with quantum bits, the name can be found after only about \sqrt{N} queries. While Grover's algorithm does not attain the exponential speedup of Shor's quantum factoring algorithm [4], it may be more versatile, by providing quadratic gains for almost any quantum algorithm [5] or accelerating NP-complete problems through exhaustive searches over possible solutions [6].

We implement the Grover search algorithm over a space of $N=4$ elements using two trapped atomic ion qubits [7, 8]. Grover's algorithm has been implemented with ensembles of molecules using nuclear magnetic resonance [9, 10, 11], with states of light using linear optical techniques [12, 13], and with Rydberg states within individual atoms [14]. None of these systems are scalable however, as they require exponential resources as the number of qubits grows. The implementation of Grover's algorithm reported here complements the repertoire of multi-qubit quantum algorithms recently demonstrated in the scalable system of trapped atomic ions [15, 16, 17, 18]. Unlike these earlier ion trap demonstrations, we use magnetically-insensitive "clock state" qubits and particular entangling gates that are uniquely suited to such qubits while remaining insensitive to external phase drifts between gates [19, 20, 21].

At the heart of Grover's algorithm is the "oracle query," which quickly checks if a proposed input " x " is a solution to the search problem. The oracle marks a particular component of a quantum superposition by flipping the sign of its amplitude. Following the oracle, a number of quantum operations amplify the weighting of the marked state independent of which state is

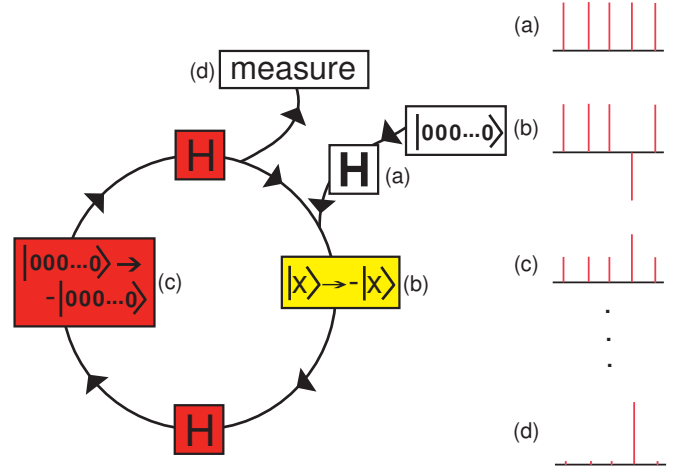


FIG. 1: Schematic diagram of Grover's quantum search algorithm over a space of n qubits ($N = 2^n$ entries). Initially, all qubits are prepared in the state $|000\dots 0\rangle$. (a) A global Hadamard gate prepares an equal superposition of all states. (b) The oracle (shaded in yellow) flips the sign of the amplitude corresponding to the marked element, represented by the n -bit binary number x . (c) Two global Hadamard gates surround an additional phase gate (shaded in red) that flips the sign of the amplitude corresponding to the initial state $|000\dots 0\rangle$, amplifying the weight of the marked state. Steps (b) and (c) are repeated in sequence a prescribed number of times, and finally (d) the qubits are measured. An example of the distributions of quantum amplitudes at each stage are depicted at the right.

marked (see Fig. 1). After many iterations of this query/amplification process, the marked state accumulates nearly all of the weight and is revealed following a measurement. The required number of queries is the integer closest to $\frac{\pi}{4 \sin^{-1}(\frac{1}{\sqrt{N}})} - \frac{1}{2}$ [22]. For $N \gg 1$, the marked element would thus appear with high probability after approximately $\pi\sqrt{N}/4$ iterations, and for the special case of $N = 4$ elements, a single query would provide the marked element with unit probability. Classically, a single query of a 4-element search space followed by a guess can only result in a successful outcome with 50%

probability.

A standard quantum circuit for the Grover search algorithm for $N=4$ entries is shown in Figure 2(a) [1]. This scheme uses a third ancilla bit which marks one of the database elements through a Toffoli gate that effectively flips the sign of the marked element if and only if the two bit input is a solution to the problem. The oracle scheme to mark each of the four possibilities is shown below the circuit. The remainder of the circuit (shaded in dark red) amplifies the weighting of the marked state, with the operations between the Hadamard gates flipping the sign of the amplitude of the $|00\rangle$ state.

Fig. 2(b) shows the experimental implementation of the algorithm for $N=4$ search elements. The Mølmer-Sørensen (M-S) entangling gate [23] is adapted to the algorithm for both the marking and state amplification steps and is accompanied by a variety of single qubit rotations. This circuit is identical in function to the circuit of Fig. 2(a) but does not use an ancilla qubit [24]. First, each qubit is initialized to the $|0\rangle$ state through optical pumping techniques. Next, an equal superposition of all qubit states is prepared with a global single qubit rotation of $\pi/2$, replacing the Hadamard gates of Figs 1 and 2(a). The oracle function (shaded in yellow) then marks one of the four possible states $|xx\rangle$ by flipping its sign. This is accomplished with a controlled-z phase gate (shaded in blue) containing the M-S gate, that flips the sign of the $|11\rangle$ state. The phase gate is surrounded by rotations (shaded in gray) that swap the marked state $|xx\rangle$ with the $|11\rangle$ state, depending on the settings of the of the rotation angles depicted in the table at the bottom of Fig 2(b). After the oracle query, a global rotation of $\pi/2$ (with a phase of $-\pi/2$ relative to the initial rotation) followed by a second application of the M-S gate amplifies the weighting of the marked state $|xx\rangle$ (operations shaded in red).

The experiment is performed with two $^{111}\text{Cd}^+$ ions confined in a three-layer linear ion trap with axial frequency $\omega_z/2\pi=2.0\text{MHz}$ [19, 20, 25]. The $S_{1/2}$ ground state hyperfine levels $|F=0, m_f=0\rangle$ (denoted by $|0\rangle$) and $|F=1, m_f=0\rangle$ (denoted by $|1\rangle$), separated in frequency by $\omega_0/2\pi=14.5\text{GHz}$, serve as qubit levels. These “clock” states are relatively insensitive to magnetic field noise, obviating the need for “spin echo” pulses in the implementation of the algorithm [16]. A variety of optical and microwave sources are used to control, entangle, and measure the qubits. In particular, pairs of off-resonant laser beams with a beatnote near ω_0 drive stimulated Raman transitions that couple the qubits to their collective motion and give rise to entangling quantum gates [20, 26]. Both the center-of-mass and stretch modes of axial motion are initialized to near the ground state via stimulated Raman cooling, with average vibrational numbers of $\bar{n}=0.28$ and 0.12 , respectively [25]. Single qubit rotations are accomplished through resonant microwave pulses (tuned to near ω_0) and composite pulse

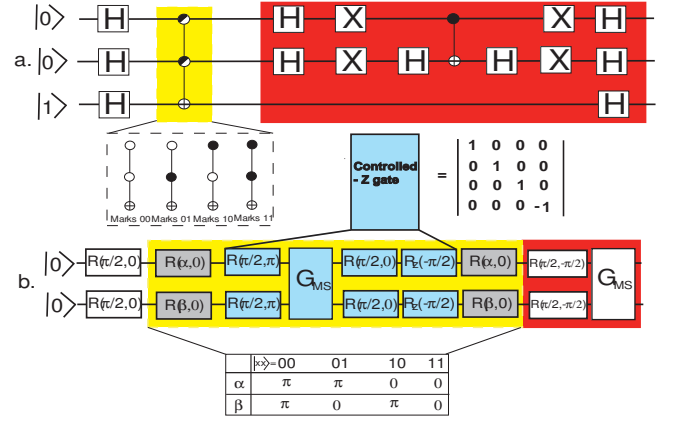


FIG. 2: Quantum circuit to implement Grover’s searching algorithm for $N=4$ entries [1]. (a.) Theoretical circuit using a third ancilla bit and standard gates including the Hadamard gate (H), the generalized Toffoli gate, a bit flip, X, and a controlled-NOT gate. The Toffoli gate implements the oracle (shaded in yellow), where the scheme to mark each of the four possibilities is shown below the circuit. The remainder of the circuit (shaded in red) amplifies the weighting of the marked state. (b.) The experimental circuit to implement the algorithm for $n=2$ qubits, where $R(\theta, \phi)$ is a rotation on the Bloch sphere [32], $R_z(\phi)$ is a phase rotation about the \hat{z} -axis, and G_{MS} is the Mølmer-Sørensen entangling gate. The yellow shaded box identifies the oracle, where the value of the variables α and β (given in the table), determine which state is marked [33]. The remainder of the circuit (shaded in red) amplifies the weighting of the marked state.

sequences involving a single tightly-focused off-resonant laser. The microwaves are applied to both qubits simultaneously and provide global single qubit rotations. The off-resonant laser, which addresses one ion more strongly than the other, creates a differential AC Stark shift between the two qubits, imparting a relative phase shift of π between the two qubits. Combined with appropriate microwave pulses, this allows arbitrary single qubit rotations. Finally, each qubit is detected with greater than 97% efficiency by uniformly illuminating the ions with resonant laser radiation and observing the ion fluorescence on an intensified CCD camera.

The Mølmer-Sørensen gate directly entangles the clock state qubits and is insensitive to the relative optical phase of the Raman laser beams between gates [19, 20, 26]. This is an important consideration when multiple entangling gates are implemented because it suppresses decoherence from magnetic fields and optical phase noise that may fluctuate from gate to gate. The M-S entangling gate is realized by applying multiple sets of Raman beatnotes to the ions, simultaneously driving the first lower and upper motional sidebands for a particular duration. This entangles the spin states via their collective motional mode, in this case the stretch mode [23]. The evolution of the four basis states is given by:

$$\begin{aligned}
|0\rangle|0\rangle &\rightarrow |0\rangle|0\rangle - i|1\rangle|1\rangle \\
|1\rangle|1\rangle &\rightarrow |1\rangle|1\rangle - i|0\rangle|0\rangle \\
|0\rangle|1\rangle &\rightarrow |0\rangle|1\rangle - i|1\rangle|0\rangle \\
|1\rangle|0\rangle &\rightarrow |1\rangle|0\rangle - i|0\rangle|1\rangle.
\end{aligned}$$

The desired states are produced with a fidelity of approximately 80%. There are additional phases not included in the above equation pertaining to the ion-ion spacing, the phase of the oscillator that defines the Raman beam beat-note, and Stark shifts from the applied Raman beams [19, 21]. These phases are set to zero for the present case since they are fixed before the experiment is run by first synchronizing the phase of the entangling gate with the phase of microwave $\pi/2$ pulses[19]. Then the phases of the two entangling gates used in the experiment are synchronized to each other through a Ramsey experiment. Note that phase noise from the Raman beam path fluctuations is suppressed due to the spectral arrangement of the Raman sidebands [20, 26]. The timescale for each operation in the algorithm is as follows: $10\mu\text{s}$ for a global microwave rotation, $20\mu\text{s}$ for a differential single qubit rotation, and $140\mu\text{s}$ for the Mølmer-Sørensen two qubit entangling gate, giving a total of $\sim 380\mu\text{s}$ to complete the 20 pulses that form the algorithm.

There are several approaches to gauging the performance of the algorithm implementation. One method is to compare the algorithm's success at recovering the marked state with the best that can be achieved classically. The classical counterpart is a simple shell game: suppose a marble is hidden under one of four shells, and after a single query the location of the marble is guessed. Under these conditions, the best classical approach gives an average probability of success $P_{cl} = 1/4 + 3/4(1/3) = 0.50$, because $1/4$ of the time the query will give the correct location of the marble while $3/4$ of the time a guess must be made amongst the three remaining choices each with $1/3$ probability of choosing the correct location. If Grover's algorithm is used, the answer to the single query would result in a 100% success rate at 'guessing' the marble's location. As can be seen in figure 3(a) the marked state is recovered with an averaged probability over the four markings of 60(2)%, surpassing the classical limit of 50%.

It is interesting to consider the output of the algorithm when the final entangling gate used for state amplification is omitted. This situation shows how well the algorithm can do with only single qubit rotations outside the oracle. This scenario lies between the classical and quantum searches described above since entanglement is not used outside the oracle but quantum superpositions are used to find the marked element. In this case it can be shown that quantum mechanics without entanglement can do no better than what can be achieved with classical means: both methods have the outcome of finding

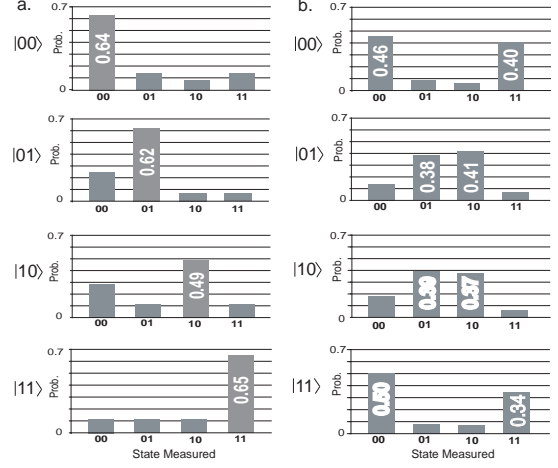


FIG. 3: (a.) Output of the algorithm. The conditional probability of measuring each of four output states given one was marked is shown in sequence from top to bottom $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Each of the four data sets shows the distribution of measurements averaged over 500 trials. The marked state was recovered on average with 60(2)%, compared to unit probability for the ideal quantum algorithm and 50% for the best possible classical algorithm. (b.) Output of the algorithm without the final entangling gate. This shows that the fidelity of the oracle is about 80%. Each of the four data sets was also averaged over 500 trials. The experimental average to recover the marked state is 41(2)% with the theoretical limit of 50%, both of which are less than the 60% from (a). The quoted errors are statistical.

the marked state with only 50% probability, assuming a perfect oracle. In addition, this diagnostic allows the performance of the oracle itself to be characterized. The rotations following the oracle convert the marked state into one of four Bell states each of which yields a maximum probability of 50% to recover the marked state. Figure 3b shows that the marked state is recovered with an average of 42(1)% probability, implying the oracle itself has a fidelity of roughly 80%.

The above figures of merit focus on the mean success probability and neglect the information content inherent in the distributions of figure 3a. The mutual information between the marking of the state and the measurement can be used to characterize this correlation and hence is another measure of the algorithm's success [1] (for other figures of merit see ref. [24]). The mutual information measures how much information two random variables, x , the measurement, and y , the marking, have in common. It is defined by: $H(x:y) = H(x) + H(y) - H(x, y)$, where $H(x, y) = -\sum_{x,y} p(x,y) \log_2 p(x,y)$ is the joint Shannon entropy between the two distributions, $p(x, y) = p(x)p(y|x)$ is the joint probability distribution of x and y , and $p(y|x)$ is the conditional probability of y having been marked given that x was measured. $H(x) = -\sum_x p(x) \log_2 p(x)$ and $H(y) = -\sum_y p(y) \log_2 p(y)$ are the Shannon entropies

of the individual variables. Classically the mutual information acquired after a single query of the oracle is $H(x:y)=0.25\log_2(0.25)-0.75\log_2(0.75)=0.81$ bits, meaning, on average, 0.81 bits of information are gained upon measurement. The ideal quantum algorithm would yield two bits of information upon measurement. For the data in fig.3a the mutual information is 0.44, so on average only about a half a bit of information is gained. Even though less information is gained per measurement than the classical case, the *probability* of finding the marked state in the experiment still exceeds the classical limit.

As the data in fig. 3a shows, the marked state is not recovered with unit probability. A large part of this infidelity is due to the Mølmer-Sørensen entangling gate. Each instance of the Mølmer-Sørensen gate has a fidelity of about 80%, and since there are two such gates in the algorithm, overall fidelities of approximately 60% are expected. The main sources of decoherence during the gate are spontaneous emission from off-resonant coupling to the excited state and fluctuating AC Stark shifts from the Raman beams that drive the entangling gate[20]. Both of these induced decoherence sources can be suppressed by increasing the detuning of the Raman beams from the excited state, at the expense of slowing the gate. We choose the detuning to strike a balance between these induced decoherence sources and other slowly varying noise sources, such as motional heating [25, 27], fluctuating magnetic fields, and microwave oscillator phase drifts. Additional power in the Raman laser beams accompanied by larger detunings could suppress decoherence from spontaneous emission and AC Stark shifts while maintaining a reasonable gate speed (see [20] for more details). Fluctuating AC Stark shifts during the differential single qubit rotations due to technical intensity fluctuations and beam pointing instabilities add infidelities to the experiment on the order of 5-10%.

For Grover's algorithm to be useful it needs to extend beyond a few qubits. Using a quantum circuit similar to fig.2a, an n -qubit Grover algorithm can be implemented with n -qubit Toffoli gates, a series of two qubit gates, and single qubit rotations. It has been shown that an n -qubit Toffoli gate can be constructed with single qubit gates and controlled-NOT gates with order n basic operations [28]. A controlled-NOT gate can be constructed from the M-S entangling gate through the following sequence [23]: $[R_2(\pi/2, 0), R_1(\pi/2, \pi), R_2(\pi/2, \pi), G_{MS}, R_1(\pi/2, 0), R_2(\pi/2, 0), R_{z1}(-\pi/2), R_{z2}(-\pi/2), R_2(\pi/2, -\pi), R_{z1}(\pi)]$, where $R_{i=1,2}(\theta, \phi)$ is a rotation of ion i by angle θ and phase ϕ , $R_{zi}(\phi)$ is a z-rotation of ion i by angle ϕ , and G_{MS} is the Mølmer-Sørensen entangling gate. Since the ion system is scalable to a large number of qubits it is feasible to construct an efficient n -qubit Grover algorithm where each iteration scales polynomially with n . In this case, the isolation of individual ions could be accomplished through tight focusing of laser beams[29]

or the shuttling of ions between separated trap zones [16, 17, 18, 30, 31].

This work is supported by the National Security Agency and Advanced Research and Development Activity under Army Research Office contract W911NF-04-1-0234, and the National Science Foundation Information Technology Research Program.

-
- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2000).
 - [2] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
 - [3] G. Brassard, Science **275**, 627 (1997).
 - [4] P. W. Shor, SIAM J. Comp. **26**, 1484 (1997).
 - [5] L. K. Grover, Proc. 30th ACM Symp. Theory Comp (ACM Press, New York, 1998), 53.
 - [6] N. J. Cerf, L. K. Grover, and C. P. Williams, Phys. Rev. A **61**, 032303 (2000).
 - [7] M. Feng, Phys. Rev. A **63**, 052308 (2001).
 - [8] C. D. Hill and H.-S. Goan, Phys. Rev. A **69**, 056301 (2004).
 - [9] I. L. Chuang, N. Gershenfeld, and M. Kubinec, Phys. Rev. Lett. **80**, 3408 (1998).
 - [10] J. A. Jones, M. Mosca, and R. H. Hansen, Nature **393**, 344 (1998).
 - [11] M. S. Anwar, *et al.*, Chem. Phys. Lett. **400**, 94 (2004).
 - [12] P. G. Kwiat, *et al.*, J. Mod. Opt. **47**, 257 (2000).
 - [13] P. Walther, *et al.*, Nature **434**, 169 (2005).
 - [14] J. Ahn, T. C. Weinacht, and P. H. Bucksbaum, Science **287**, 463 (2000).
 - [15] M. Riebe, *et al.*, Nature **429**, 734 (2005).
 - [16] M. D. Barrett, *et al.*, Nature **429**, 727 (2005).
 - [17] T. Schaetz, *et al.*, Phys. Rev. Lett. **93**, 040505 (2004).
 - [18] J. Chiaverini, *et al.*, Science **308**, 997 (2005).
 - [19] P. C. Haljan *et al.*, Phys. Rev. Lett. **94**, 153602 (2005).
 - [20] P. C. Haljan *et al.*, quant-ph/0508123, (2005).
 - [21] P. J. Lee *et al.*, quant-ph/0505203.
 - [22] M. Boyer, *et al.*, Fortschritte der Physik **46**, 493 (1998).
 - [23] A. Sørensen and K. Mølmer, Phys. Rev. Lett. **82**, 1971 (1999).
 - [24] J. L. Dodd, T. C. Ralph, and G. J. Milburn, Phys. Rev. A **68**, 042328 (2003).
 - [25] L. Deslauriers *et al.*, Phys. Rev. A **70**, 043408 (2004).
 - [26] P. J. Lee *et al.*, Opt. Lett. **28**, 1582 (2003).
 - [27] Q. Turchette *et al.*, Phys. Rev. A **61**, 063418 (2000).
 - [28] A. Barenco, *et al.*, Phys. Rev. A **52**, 3457 (1995).
 - [29] F. Schmidt-Kaler, *et al.*, Nature **422**, 408 (2003).
 - [30] M. A. Rowe, *et al.*, QIC **2**, 257 (2002).
 - [31] D. Kielpinski, C. Monroe, and D. J. Wineland, Nature **417**, 709 (2002).
 - [32] Under this convention the basis states evolve as: $|0\rangle \rightarrow \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$ and $|1\rangle \rightarrow -e^{-i\phi}\sin(\theta/2)|0\rangle + \cos(\theta/2)|1\rangle$
 - [33] In the experiment the first set of rotations (shaded in gray) are accompanied by extra z-rotations. These additional phases do not affect the outcome of the oracle and are suppressed in the figure for simplicity.